Security of Binary Modulated Continuous Variable Quantum Key Distribution under Collective Attacks

Yi-Bo Zhao[1], Matthias Heid[2,3], Johannes Rigas[4], and Norbert Lütkenhaus[2,3]

[1]*Key Lab of Quantum Information, University of Science and Technology of China, (CAS), Hefei, Anhui 230026, China*
[2] *Quantum Information Theory Group, Institut für Theoretische Physik I,*
& Max-Planck Research Group, Institute of Optics, Information and Photonics,
Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany
[3] *Institute for Quantum Computing & Department of Physics and Astronomy,*
University of Waterloo, 200 University Ave. W. N2L 3G1, Canada
[4] *Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain*

We give an achievable secret key rate of a binary modulated continuous variable quantum key distribution schemes in the collective attack scenario considering quantum channels that impose arbitrary noise on the exchanged signals. Bob performs homodyne measurements on the received states and the two honest parties employ a reverse reconciliation procedure in the classical post-processing step of the protocol.

PACS numbers:

I. INTRODUCTION

Quantum key distribution (QKD) is a way to establish a key between two communicating parties, traditionally called Alice and Bob, which is provable secure against any eavesdropping strategy of an technologically unlimited third party Eve. In principle, Alice and Bob can achieve this goal by exchanging nonorthogonal quantum states as signals and using non-commuting measurements on the receiver side. Any eavesdropper needs to interact with these quantum signals to gain information about the sent signal. This inevitably causes a disturbance of the signals and leads to errors in the data that Alice and Bob observe. If the amount of errors lies below a certain threshold, Alice and Bob proceed by post-processing their data: they correct for errors and employ privacy amplification to cut out any residual information that Eve might have with the raw key. In this article, we give a lower bound to the secret key rate of a continuous variable (CV) QKD scheme [1, 2, 3, 4] employing homodyne detection in the collective attack scenario. As the outcomes of Bob's measurement are continuous, it is convenient to characterize Eve's interference with the signal states by the first and second moments of Bob's measurement outcomes. These parameters are usually given in terms of the observed loss and the excess noise of the quantum channel connecting Alice and Bob. The proof technique presented here can be used to compute secret key rates of a binary modulated CV-QKD scheme for arbitrary, in particular non-Gaussian observations, thereby extending the results given in [3]. This is important from a conceptual point of view, as the optimality of Gaussian attacks [5, 6] has only been shown for CV-schemes using a Gaussian modulated set of coherent states as input [4, 7, 8]. So far, the security of the binary scheme is not fully established yet, even if one limits the eavesdropper to collective attacks. Our analysis presented here is restricted to the asymptotic key limit as the number of exchanged signals n approaches infinity.

We consider the class of collective attacks [9, 10], thereby limiting Eve's possible interaction with the signal states. In this scenario, Eve can only interact with each signal individually, but she can store these quantum states for later usage. In the classical post-processing phase, Alice and Bob exchange information about their shared bit strings over a authenticated classical channel. This information eventually leaks to Eve, who can make use of this additional knowledge to employ optimized measurement on her quantum states. Our starting point of the security estimation presented here is to assume that the quantum state effectively shared by Alice, Bob and Eve, is of product form $\rho_{ABE}^{\otimes n}$. In contrast to that, the most general coherent attacks can introduce correlations between the quantum states describing subsequent signals. However, it is known that this kind of attack does not give any advantage to Eve in the asymptotic key limit, if the local dimension of the involved Hilbert spaces are finite [11]. Unfortunately, the quantum de Finetti theorem cannot be directly applied here, as one needs to bound the local dimension of Bob's received states, which generally is infinite dimensional in CV-QKD. Recent work [12] indicates that there is hope that one can extend this results to the infinite dimensional case.

The experimental feasibility of various CV-QKD schemes using coherent states as input and variations of homodyne detection has already been demonstrated [7, 8, 13, 14, 15, 16, 17]. Although promising from a technological point of view as the measurement can operate at high repetition rates, the efficiency of these schemes seems to be limited by the classical post-processing protocol. In general, the performance can be improved by using reverse reconciliation (RR): one reverses the flow of classical information in the error-correction step of the protocol, so that the raw key is based upon Bob's measurement results [7]. If a practical error-correction procedure with non-ideal efficiency is considered, additional procedures like postselection [18] might become favorable to increase the efficiency [3]. Here, we limit ourselves to the idealized scenario of CV-QKD involving noiseless detectors and perfect error-correction. Consequently, we suppose that a RR protocol without postselection procedures is used. The aim is to present the still missing security analysis for a discrete modulated CV-QKD valid in an idealized setting but considering arbitrary noise in the collective attack scenario. It should also be noted that in a typical physical realization, Alice sends an additional phase reference pulse to Bob via Eve's domain. In general, Eve could interact with this additional mode as well to gain more information about the exchanged signals. As shown by Häseler *et al.* [19], a full security proof would have to take the full two mode structure of the signals into account, but also additional measurements have to be done to test the reference-signal structure of the two modes. Here, we present a simplified proof and assume that Bob's phase reference is prepared locally. Consequently, our signals are single modes.

Typical experiments show that the dominant contribution to the excess noise in CV-QKD is due to the electronic noise of the detectors [15]. Therefore, we expect the channel excess noise relevant in CV-QKD to be relatively low and of the order of a few percent. Our analysis is based on work done by Rigas [20], who gave an estimation of the maximal eigenvalues and corresponding eigenstates of a quantum state based on homodyne detection. In our protocol, Alice uses coherent states as signals. If the quantum channel imposes loss onto the signals, but is noiseless otherwise, Bob's received states ρ_B^x, conditioned on Alice sending the bit-value x, are pure coherent states. In contrast to that, Bob will receive mixed conditional states if the quantum channel imposes additional noise upon the signals. Consequently, the maximal eigenvalue of the received states ρ_B^x will deviate from unity as $1 - \tilde{\varepsilon}_x$. In this article, we use $\tilde{\varepsilon}_x$ together with the overlap of the corresponding eigenstates $\tilde{\varepsilon}_x$ as a figure of merit to quantify the amount excess noise present in the quantum channel. These parameters will be connected to the observed measurement outcomes of Alice and Bob in Sec. V. For $\tilde{\varepsilon}_x = 0$, we retrieve the known results for the lossy channel given in Ref. [3]. Therefore, we expect our approach to yield positive key rates as long as the noise of the quantum channel and consequently $\tilde{\varepsilon}_x$ is small enough.

This article is organized as follows: In the next section, we introduce a binary CV-QKD protocol where Bob is allowed to coarse grain his continuous measurement outcomes to discrete bit-values arbitrarily, which will be used as the raw key. Therefore, we modify the known security analysis for collective attacks to include this additional step in Sec. III. Then, we proceed by computing the secret key rate of a binary CV-QKD protocol with a fixed discretization of the continuous measurement outcomes. This will be done in two steps: in Sec. IV, we give an expression for the secret key rate in terms of maximal eigenvalues and corresponding eigenstates of Bob's received conditional states. These parameters are then estimated via Bob's homodyne measurement in the proceeding section. We conclude with a numerical evaluation of the secret key rate in a experimental relevant scenario and a discussion of the results.

II. THE PROTOCOL

We consider a prepare-and-measure protocol using continuous variable states and homodyne detection. In general, we allow Bob to discretize his continuous measurement outcomes and to do announcements arbitrarily. However, we also give a description of a concrete protocol as an example with those steps specified. This specific protocol will be used in Sec. VI to evaluate the secret key rate for a typical experiment numerically. Any QKD protocol can be decomposed into two phases. In the first phase Alice prepares quantum states and sends them to Bob, who then performs measurements on them. In the second phase, Alice and Bob use an authenticated two-way channel for classical communication to turn the classical data (knowledge of signals sent, and measurement results) into a secret key.

Quantum phase:

1. Alice sends a sequence of coherent states with amplitude α but randomly selected opposing phase, $|\alpha\rangle$ or $|-\alpha\rangle$, to Bob. Alice stores her choice for signal i in a variable x_i by assigning to the choice $|\alpha\rangle$ the value $x_i = 1$, and to $|-\alpha\rangle$ to $x_i = 0$.

2. Bob randomly measures each signal with a homodyne measurement corresponding to the q or p quadratures [18]. We denote Bob's measurement results as y_i and denote the basis choice by the binary variable b_i (We choose the reference frame such that the signal states are modulated in the q quadratures.

Classical phase:

3. After the quantum phase, Bob announces for each signal the measurement basis.

4. Alice and Bob test their correlations by publishing randomly selected data points x_i and y_i. Moreover all of their data (Alice's modulation and Bob's full measurement result) that originated from Bob measuring the p quadrature is published and used to check for Eve's interference.

5. Alice and Bob dismiss the data that originated from measuring in the p basis for the remaining key distillation part of the protocol in order to obtain the sifted key.
6. Let us denote the string of outcomes pertaining to the sifted key as $\{\vec{x}, \vec{y}\}$. From the collection of outcomes $\vec{y}$ Bob computes a string $\vec{u}$ and $\vec{\tilde{y}}$ to that we will refer to as the *announcement* and the *discretization* in the following.
7. Bob announces $\vec{u}$ and keeps $\vec{\tilde{y}}$. In general, the announced vector $\vec{u}$ will have continuous entries. Bob could, for example, announce the modulus $|y_i|$ of his measurement result, whenever he chose the q-quadrature as basis. The discretization $\vec{\tilde{y}}$ is vector with discrete entries from which the secret key will be generated. This could be, for example, the sign of Bob's outcomes y_i whenever he measured the q-quadrature.
8. Bob sends Alice error correction information to allow her to reconcile her string $\vec{x}$ of the sifted data to the corresponding string $\vec{\tilde{y}}$.
9. Alice and Bob do privacy amplification by applying universal-2 hash functions to the string $\vec{\tilde{y}}$, now shared by Alice and Bob. This will effectively shorten the string $\vec{\tilde{y}}$ by $n\tau$ bits of information, where n is number of transmitted signals.

This protocol is equivalent to an entanglement based protocol [21]. In step 1, Alice prepares a entangled state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|-\alpha\rangle + |1\rangle|\alpha\rangle)$ and sends the coherent state system to Bob. Then she measures her state in the $|0\rangle$ and $|1\rangle$ basis. Steps 2 to 9 remain the same.

III. THE SECRET KEY RATE IN THE INFINITE KEY LIMIT

Our security analysis follows the one given in Ref. [9, 10]. Here, we limit ourselves to the asymptotic key limit as the number of entries n in the raw key $\vec{y}$ tend to infinity. Therefore, we only consider leading terms in n in the formulas. Let $\mathbf{X}$, $\mathbf{Y}$, $\tilde{\mathbf{Y}}$ and $\mathbf{U}$ denote random variables that can take the values $\vec{x}$, $\vec{y}$, $\vec{\tilde{y}}$, $\vec{u}$ as introduced in the preceding section. In step 6 of our protocol, Bob announces $\vec{u}$, so that this information becomes available to both Alice and Eve. The classical information contained in the announcement can be formally embedded in a quantum system $\rho_{\mathbf{U}}$. After the announcement, the system $\rho_{\mathbf{XU}}$ describes Alice's data and $\rho_{E\mathbf{U}}$ describes the state Eve holds. Later in the step 8 of the protocol Bob sends error correction information over the public channel to Alice. As Eve can listen to this channel, the information W about the key contained in the error correction becomes available to her. Again, we can formally embed this classical information in a quantum state $\rho_{\mathbf{W}}$. After the error correction, Alice and Bob share $\vec{\tilde{y}}$ and Eve's knowledge about the exchanged data is summarized in a state $\rho_{E\mathbf{UW}}$. According to Ref. [22] one has to shrink the raw key by $n\tau = S(\tilde{\mathbf{Y}} : E\mathbf{UW})$ bits of information in the asymptotic key limit, where S denotes the quantum mutual information [23], so that the final key will be secure with high probability. The secret key rate that Alice and Bob finally can obtain is given by $H(\tilde{\mathbf{Y}}) - n\tau$, where $H(\tilde{\mathbf{Y}})$ describes the Shannon entropy of $\tilde{\mathbf{Y}}$, which can be evaluated after the channel test. From Ref. [9] we know that

$$n\tau = S(\tilde{\mathbf{Y}} : E\mathbf{UW}) \leq S(\tilde{\mathbf{Y}} : E\mathbf{U}) + I(\tilde{\mathbf{Y}} : \mathbf{W}), \quad (1)$$

where I denotes the Shannon mutual information [24]. Alice has to correct all the errors in her string $\vec{x}$ in step 8 of the protocol. Therefore, Bob sends Alice error correction information. The amount of error correction information necessary for Alice to succeed is given by

$$I(\tilde{\mathbf{Y}} : \mathbf{W}) = f(e)[H(\tilde{\mathbf{Y}}) - I(\mathbf{XU} : \tilde{\mathbf{Y}})], \quad (2)$$

where $f(e) \geq 1$ denotes the efficiency of the error correction procedure. Alice and Bob know the amount of published error correction information after step 8. In the following, we assume that the error correction is ideal, so that $f(e) = 1$. From the Eqs. (1,2) we know that we have to shrink the key in the privacy amplification step by

$$n\tau \leq S(\tilde{\mathbf{Y}} : E\mathbf{U}) + H(\tilde{\mathbf{Y}}) - I(\mathbf{XU} : \tilde{\mathbf{Y}}),$$

bits of information. The length of the final secret key that Alice and Bob can obtain is given by

$$\begin{aligned} nG &= H(\tilde{\mathbf{Y}}) - n\tau & (3)\\ &\geq I(\mathbf{XU} : \tilde{\mathbf{Y}}) - S(E\mathbf{U} : \tilde{\mathbf{Y}}) \\ &= I(\mathbf{X} : \tilde{\mathbf{Y}}|\mathbf{U}) - S(E : \tilde{\mathbf{Y}}|\mathbf{U}) . \end{aligned}$$

In the third line we have used the result that $S(UV : W) = S(U : W|V) + S(V : W)$, which also holds for the classical mutual information $I(UV : W)$ in particular. The length of the secret key can be lower bounded as

$$\begin{aligned} nG &= I(\mathbf{X} : \tilde{\mathbf{Y}}|\mathbf{U}) - S(E : \tilde{\mathbf{Y}}|\mathbf{U}) \\ &= I(\mathbf{X} : \tilde{\mathbf{Y}}|\mathbf{U}) - S(E|\mathbf{U}) + S(E|\mathbf{U}\tilde{\mathbf{Y}}) \\ &\geq I(\mathbf{X} : \tilde{\mathbf{Y}}|\mathbf{U}) - S(\mathbf{Y} : E) , & (4) \end{aligned}$$

where we have used the definition of the quantum mutual information $S(E : \tilde{\mathbf{Y}}|\mathbf{U})$ in the second line. The third line follows from the concavity of the entropy [23] as we will explain now. After Alice's and Bob's measurements, Eve's knowledge about the exchanged data is summarized in conditional quantum states $\rho_E^{\vec{x},\vec{y}}$. Eve's states conditioned on Bob's measurement outcomes y are therefore given by

$$\rho_E^{\vec{y}} = \sum_{\vec{x}} P(\vec{x}|\vec{y})\rho_E^{\vec{x},\vec{y}} . \quad (5)$$

From the measured outcomes $\vec{y}$, Bob computes the announcement $\vec{u}$ and the discretization $\vec{\tilde{y}}$. This can be modelled by a classical channel described by some given conditional probability distribution $P\left(\vec{y}|\vec{u}\right), \vec{\tilde{y}}$. The state $\rho_E^{\vec{u},\vec{\tilde{y}}}$ can therefore be written as

$$\rho_E^{\vec{u},\vec{\tilde{y}}} = \sum_{\vec{y}} P\left(\vec{y}|\vec{u},\vec{\tilde{y}}\right)\rho_E^{\vec{y}} \; . \tag{6}$$

It follows that the conditional entropy $S(E|\mathbf{U}\tilde{\mathbf{Y}})$ can be bounded from below as

$$\begin{aligned} S(E|\mathbf{U}\tilde{\mathbf{Y}}) &= \sum_{\vec{\tilde{y}}} \int d\vec{u} P(\vec{u},\vec{\tilde{y}}) S\left(\rho_E^{\vec{u},\vec{\tilde{y}}}\right) \\ &= \sum_{\vec{\tilde{y}}} \int d\vec{u} P(\vec{u},\vec{\tilde{y}}) S\left(\int d\vec{y} P\left(\vec{y}|\vec{u},\vec{\tilde{y}}\right)\rho_E^{\vec{y}}\right) \\ &\geq \sum_{\vec{\tilde{y}}} \int d\vec{u} P(\vec{u},\vec{\tilde{y}}) \int d\vec{y} P\left(\vec{y}|\vec{u},\vec{\tilde{y}}\right) S(\rho_E^{\vec{y}}) \\ &= \sum_{\vec{y}} P(\vec{y}) S(\rho_E^{\vec{y}}) = S(E|\mathbf{Y}) \; , \end{aligned} \tag{7}$$

where we first used Eq. (6) and then the concavity of the entropy. Since the conditional entropy $S(E|\mathbf{U})$ obeys $S(E|\mathbf{U}) \leq S(E)$ by the concavity of the entropy [23], the last line of Eq.(4) follows with the help of Eq. (7).

The lower bound in Eq. (4) has two terms, one depending on the discretization $\tilde{\mathbf{Y}}$, one independent of it. We expect to be able to find a discretization for arbitrary correlations between Alice and Bob, so that the first term goes to $I(\mathbf{X}:\mathbf{Y})$, e.g. a family of discretizations $\tilde{\mathbf{Y}}_\Delta$ that tend to the identity $\tilde{\mathbf{Y}}_\Delta \rightarrow \mathbf{Y}$ asymptotically as $\Delta \rightarrow 0$. Here, the parameter Δ describes the size of the coarse-graining of continuous measurement outcomes to a certain discrete value. In Sec. VI we will give a simple example of a discretization that can achieve the bound $I(\mathbf{X}:\mathbf{Y})$ for particular class of correlations between Alice and Bob without an asymptotic procedure.

In the following, we limit our security analysis to the collective attack scenario and assume that the total state shared by Alice, Bob and Eve has tensor product form $\rho_{ABE}^{\otimes n}$. Thus, the measurement outcomes x_i and y_i are independently identical distributed, and we can limit ourselves to single letter distributions. Then, Bob computes $\tilde{y}$ and announces values u from his measured value of y. Therefore, Eq. (4) can be simplified as

$$G \geq I(X:\tilde{Y}|U) - S(Y:E) \; , \tag{8}$$

where we have introduced the single letter random variables X, Y, $\tilde{Y}$ and U that can take the values x, y, $\tilde{y}$ and u respectively. The remaining central problem is to find a upper bound to $S(E:Y)$ as the first term is already available from the observed outcomes. Without loss of the generality, we can assume Eve holds the purification of ρ_{ABE}. Define the set $\Xi_{ABE}(\rho)$ as a collection of all of the possible pure state ρ_{ABE} that compatible with the observations available from the measurement. The secret key rate is then given by

$$G \geq I(X:\tilde{Y}|U) - \max_{\rho_{ABE}\in\Xi_{ABE}(\rho)} S(Y:E). \tag{9}$$

In this article, we calculate this expression (9) for the binary modulated CV-QKD scheme introduced in Sec. II. This will be done as follows: first, we will divide the entropy $S(Y:E)$ into three terms. Then we will give an upper bound to each term independently. These bounds can either be directly given by Bob's observed first and second moments or can be expressed as functions of the maximal eigenvalues and corresponding eigenstates of Eve's conditional states. We conclude our proof by estimating these parameters via the first and second moments of Bob's homodyne measurements using the results of Ref. [20] combined with an argument based on Schmidt's decomposition. In the last section we evaluate the expected secret key rate G for typical observations numerically.

IV. LOWER BOUND ON THE SECRET KEY RATE

The central problem of calculating the secret key rate in a reverse reconciliation scheme according to Eq. 9 is to find an upper bound for the mutual information $S(Y:E)$ that can be estimated by observable quantities. This will be done in the following. As the mutual information between Alice and Eve is given by

$$S(X:E) = S(E) - S(E|X) \; ,$$

one can express the quantum mutual information $S(Y:E)$ between Bob and Eve in Eq.(9) as

$$S(Y:E) = S(E|X) + S(X:E) - S(E|Y) \; . \tag{10}$$

As already mentioned, we will proceed to calculate an upper bound for $S(Y:E)$ by bounding the three terms $S(E|X)$, $S(X:E)$ and $S(E|Y)$ on the right hand side of Eq. (10) individually. As we will see later, we can directly compute an upper bound for $S(E|X)$ from Bob's observed data. The remaining two terms will be given as functions of the maximal eigenvalues $1-\tilde{\varepsilon}_x$ and corresponding eigenstates $|\tilde{\varepsilon}_x\rangle$ of Eve's conditional states ρ_E^x.

In Ref. [20], Rigas presented an estimation of the maximal eigenvalue and corresponding eigenstate of an unknown quantum state based on the first and second moments of a homodyne measurement. We use this result to estimate the biggest eigenvalue $1-\tilde{\varepsilon}_x$ and corresponding eigenstate $|\tilde{\varepsilon}_x\rangle$ of Eve's conditional states ρ_E^x via Bob's measurements. We can express Eve's conditional states using this notation as

$$\rho_E^x = (1-\tilde{\varepsilon}_x)|\tilde{\varepsilon}_x\rangle\langle\tilde{\varepsilon}_x| + \tilde{\varepsilon}_x\sigma_E^x \; , \tag{11}$$

where $|\tilde{\varepsilon}_x\rangle\langle\tilde{\varepsilon}_x|$ have σ_E^x orthogonal support. We will refer to the eigenstate belonging to the maximal eigenvalue as the maximal eigenstate.

In the following, we will assume that the maximal eigenvalues $1-\tilde{\varepsilon}_x$ and eigenvectors $|\tilde{\varepsilon}_x\rangle$ are given. Section V contains an estimation of these parameters from measurement data and will conclude our approach.

It turns out that an upper bound for Eve's conditional entropy $S(E|X)$, the first term on the right hand side of Eq. (10), can be obtained by exploiting Gaussian extremality properties [25]. The second term is the mutual information between Alice and Eve $S(X:E)$, which can be upper bounded by employing a suitable purification method. The estimation of the third term, the entropy $S(E|Y)$ conditioned on Bob's measurement outcomes Y is technically more involved and includes a linearization of the respective quantities, so that a bound can be evaluated.

A. Eve's entropy $S(E|X)$ conditioned on Alice's variable X

For given first and second moments of Bob's measurement outcomes, we have to find an upper bound for Eve's conditional entropy $S(E|X)$, which is the first term on the right hand side of Eq. (10). The *a priori* probabilities $P(x)$ are fixed by Alice's state preparation. In the entanglement based description of the protocol, Alice's state preparation is equivalent to projection measurement onto her A system of a pure three party state ρ_{ABE}. It follows that the combined two party state $\rho_{EB}^x = |\Psi_{BE}^x\rangle\langle\Psi_{BE}^x|$ between Eve and Bob conditioned on Alice's measurement outcome x is pure. Therefore, by Schmidt's decomposition, we conclude that $S(\rho_E^x)=S(\rho_B^x)$ [23]. It is known that the state with maximal entropy $S(\rho_B^x)$ for fixed first and second moments is Gaussian [25, 26]. Since $S(\rho_E^x)=S(\rho_B^x)$ and $P(x)$ is fixed, one can directly apply the result given in Eqs. (15) and (16) of Ref. [26], so that

$$\begin{aligned} S(E|X) &= \sum_x P(x) S(\rho_E^x) \qquad (12)\\ &\leq \frac{1}{2}\sum_x [(1+V_x)\log_2(1+V_x) - V_x \log_2 V_x] \, . \end{aligned}$$

The term

$$V_x = \sqrt{V_{Y_q|x}^2 V_{Y_p|x}^2} - 1/2 \qquad (13)$$

quantifies the amount of excess noise imposed by the quantum channel connecting Alice and Bob. It is a function of Bob's observed variances $V_{Y_q|X}^2$ and $V_{Y_p|X}^2$ of the corresponding quadrature distributions, that are given by

$$\begin{aligned} V_{Y_q|X}^2 &= \mathrm{tr}\left(\rho_B^x \hat{q}^2\right) - \left[\mathrm{tr}\left(\rho_B^x \hat{q}\right)\right]^2 \qquad (14)\\ V_{Y_p|X}^2 &= \mathrm{tr}\left(\rho_B^x \hat{p}^2\right) - \left[\mathrm{tr}\left(\rho_B^x \hat{p}\right)\right]^2 \, , \qquad (15) \end{aligned}$$

and the quadrature operators $\hat{q}$ and $\hat{p}$ are defined as

$$\begin{aligned} \hat{q} &= \frac{1}{\sqrt{2}}\left(\hat{a}+\hat{a}^\dagger\right) \qquad (16)\\ \hat{p} &= \frac{\mathrm{i}}{\sqrt{2}}\left(\hat{a}-\hat{a}^\dagger\right) \, , \end{aligned}$$

whereas $\hat{a}$ and $\hat{a}^\dagger$ denote the photon annihilation and creation operators.

B. The mutual information $S(X:E)$ between Alice and Eve

Here, we employ methods known from state estimation to calculate the mutual information term $S(X:E)$ between Alice and Eve in Eq. (10). After interacting with the signal states, Eve holds the conditional states ρ_E^x in her ancilla system, that she wants to distinguish optimally in order to maximize the mutual information $S(X:E)$. If we introduce an auxiliary system Q that contains a purification of the states ρ_E^0 and ρ_E^1, we can give an upper bound for $S(X:E)$: the mutual information can never increase when discarding subsystems, so that

$$S(X:E) \leq S(X:QE) \qquad (17)$$

holds. We choose the purification Q, so that the conditional states ρ_E^x are purified as $|\Psi_{EQ}^x\rangle$. There are certainly purifications that would leak too much information to Eve, i.e. if one would supply Eve with a purification of the global state ρ_{XQE}. Since Eq.(17) is valid for any purification, we would ideally choose one that minimizes $S(X:QE)$ to make the bound (17) as tight as possible. This problem is closely connected to Uhlmann's theorem, as we will show now.

It has been shown that the quantum mutual information between a classical register described by the binary variable X and a quantum system QE can be expressed as

$$S(X:QE) = h\left[\frac{1}{2}\left(1-|\langle\Psi_{EQ}^0|\Psi_{EQ}^1\rangle|\right)\right] , \qquad (18)$$

if the conditional states $|\Psi_{EQ}^x\rangle$ are pure [3]. Here, h denotes the binary entropy function

$$h(z) = -z\log_2 z - (1-z)\log_2(1-z) \, . \qquad (19)$$

Since $S(X:EQ)$ monotonously increases with decreasing overlap $|\langle\Psi_{EQ}^0|\Psi_{EQ}^1\rangle|$, it is sufficient to find the purification Q that maximizes the overlap $|\langle\Psi_{EQ}^0|\Psi_{EQ}^1\rangle|$ to minimize $S(X:EQ)$. The solution to this problem is known as Uhlmann's theorem [23]:

$$F\left(\rho_E^0,\rho_E^1\right) = \max_{|\Psi_{EQ}^0\rangle,|\Psi_{EQ}^1\rangle} |\langle\Psi_{EQ}^0|\Psi_{EQ}^1\rangle| \qquad (20)$$

Here, the Uhlmann fidelity $F\left(\rho_E^0, \rho_E^1\right)$ is defined as

$$F\left(\rho_E^0, \rho_E^1\right) = \mathrm{tr}_{\mathrm{E}}\left(\sqrt{\sqrt{\rho_E^0}\rho_E^1\sqrt{\rho_E^0}}\right) . \tag{21}$$

Therefore, we conclude that the tightest bound obtainable from Eq. (17) to mutual information $S(X:QE)$ for a binary modulated setup is given by Eq. (20) and Eq. (18) as

$$S(X:E) \leq h\left[\frac{1}{2}\left\{1 - F\left(\rho_E^0, \rho_E^1\right)\right\}\right] \tag{22}$$

In general, the upper bound (22) of the mutual information $S(X:E)$ can be calculated, if the Eve's conditional states ρ_E^x are known. However, the full information about the states ρ_E^x is usually not available from measurements. As already mentioned, we base our security analysis on the estimation of the maximal eigenvalues $1 - \tilde{\varepsilon}_x$ and corresponding eigenstates $|\tilde{\varepsilon}_x\rangle$ of Eve's conditional states ρ_E^x that we will estimate by Alice and Bob's observation. Therefore, we proceed by giving an upper bound of $S(X:E)$ as function of these parameters. This can be done by by considering a particular purification Q.

Any purification $|\Psi_{EQ}^x\rangle$ can be expanded as

$$|\Psi_{EQ}^x\rangle = \sum_i c_i^x |i_Q^x\rangle|i_E^x\rangle . \tag{23}$$

Without loss of generality, we can choose the first term in the Schmidt-decomposition (23) to correspond to the maximal eigenvalue $c_0^{x\,2} := 1 - \tilde{\varepsilon}_x$. The corresponding eigenstate is then given by Eq. (11) as $|0_E^x\rangle = |\tilde{\varepsilon}_x\rangle$. With the help of expansion (23), the modulus of the overlap between the two conditional states can be evaluated as

$$\left|\langle\Psi_{EQ}^0|\Psi_{EQ}^1\rangle\right| = \left|\sum_{ij} c_i^0 c_j^1 \langle i_i^0|j_Q^1\rangle\langle i_E^0|j_E^1\rangle\right| . \tag{24}$$

If one chooses $\langle i_Q^0|j_Q^1\rangle = \delta_{ij}e^{i\varphi_i}$, where δ_{ij} is the Kronecker delta function and the phase φ_i is the negative of the phase of the complex number $\langle i_E^0|i_E^1\rangle$, it follows that

$$\begin{aligned} \left|\langle\Psi_{EQ}^0|\Psi_{EQ}^1\rangle\right| &= \left|\sum_i c_i^0 c_i^1 e^{i\varphi_i}\langle i_E^0|i_E^1\rangle\right| \qquad (25) \\ &\geq \sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}\,|\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle| . \end{aligned}$$

Therefore, we obtain a lower bound on the quantum mutual information $S(X:E)$ using Eq. (18) and Eq. (25) as

$$\begin{aligned} S(X:E) &\leq S(X:QE) \qquad (26) \\ &\leq h\left[\frac{1}{2}(1 - \sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}\gamma)\right] , \end{aligned}$$

where we introduced

$$\gamma := |\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle| , \tag{27}$$

as a short hand notation for the overlap of Eve's maximal eigenstates. In Sec. V we will estimate the values for $\tilde{\varepsilon}_x$ and γ via Bob's homodyne measurements.

C. Eve's entropy $S(E|Y)$ conditioned on Bob's measurement outcome Y

The last term of Eq. (10) to be estimated reads

$$S(E|Y) = \int dy P(y) S(\rho_E^y) . \tag{28}$$

Prior to Alice's measurement, the three party state ρ_{ABE} can be assumed to be pure. Since Alice performs a projection measurement on her subsystem, it follows that the combined two party state $\rho_{EB}^x = |\Psi_{BE}^x\rangle\langle\Psi_{BE}^x|$ between Eve and Bob conditioned on Alice's measurement result is pure. Moreover, Bob performs a projection measurement $|y\rangle\langle y|$ on his subsystem, so that Eve's state $|\Psi_E^{xy}\rangle$ conditioned on Alice's measurement outcome x and Bob's outcome y is pure. Eve's states ρ_E^y conditioned on Bob's measurement outcome y can be written as

$$\rho_E^y = P(0|y)|\Psi_E^{0y}\rangle\langle\Psi_E^{0y}| + P(1|y)|\Psi_E^{1y}\rangle\langle\Psi_E^{1y}| . \tag{29}$$

From Sec. III.C of Ref. [3] we know that

$$\begin{aligned} S(\rho_E^y) &= h\left[\frac{1}{2} - \frac{1}{2}\sqrt{1 - 4P(0|y)P(1|y)(1 - |\langle\Psi_E^{0y}|\Psi_E^{1y}\rangle|^2)}\right] \\ &= g\left(P(0|y), \left|\langle\Psi_E^{0y}|\Psi_E^{1y}\rangle\right|\right) , \qquad (30) \end{aligned}$$

where we have introduced the function $g\left(P(0|y), \left|\langle\Psi_E^{0y}|\Psi_E^{1y}\rangle\right|\right)$ as a shorthand notation. As we can see, the entropy $S(E|Y)$ to be evaluated is a function of the overlaps

$$\Gamma_y = \left|\langle\Psi_E^{0y}|\Psi_E^{1y}\rangle\right| , \tag{31}$$

that depend on the outcomes y. Additionally, the probability distributions $P(0|y)$ and $P(y)$ need to be estimated by the channel test. We will proceed to lower bound the entropy $S(E|Y)$ (28) by exploiting special properties of the g function given by equation (30). It can be easily verified that $g\left(P(0|y), \Gamma_y\right)$ as a function of the overlaps has the following properties:

$$g(P(0|y), 1) = 0 \tag{32}$$

$$\frac{\partial g(P(0|y), x)}{\partial x} \leq 0 \tag{33}$$

$$\frac{\partial^2 g(P(0|y), x)}{\partial x^2} \leq 0 \tag{34}$$

We introduce positive and real parameters γ_y and $\Delta\gamma_y$ such that we can rewrite the overlap Γ_y (31) as

$$\Gamma_y \leq \gamma_y + \Delta\gamma_y . \tag{35}$$

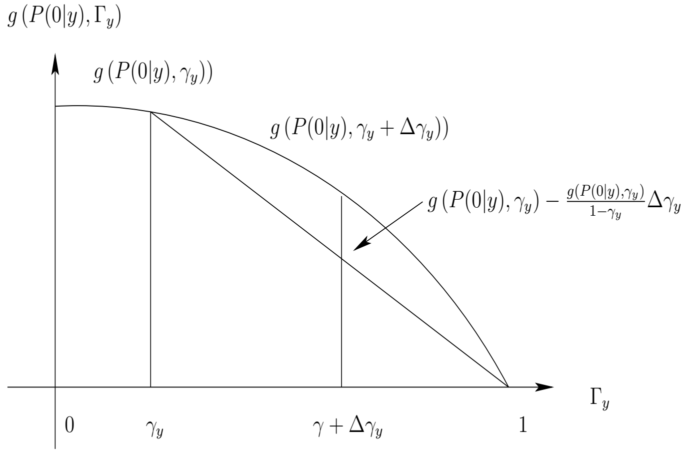
$g\,(P(0|y),\Gamma_y)$
$g\,(P(0|y),\gamma_y))$
$g\,(P(0|y),\gamma_y+\Delta\gamma_y))$
$g\,(P(0|y),\gamma_y)-\frac{g(P(0|y),\gamma_y)}{1-\gamma_y}\Delta\gamma_y$
Γ_y
0
γ_y
$\gamma+\Delta\gamma_y$
1

FIG. 1: Schematical representation of the function $g\,(P(0|1),\Gamma_y)$.The validity of Eq. (36) can easily be checked for all $\Gamma_y \leq \gamma_y + \Delta\gamma_y$.

It follows that for any $0 \leq \Gamma_y \leq 1$ the inequality

$$\begin{aligned} g(P(0|y),\Gamma_y) &\geq g(P(0|y),\gamma_y+\Delta\gamma_y) \\ &\geq g(P(0|y),\gamma_y) - \frac{g(P(0|y),\gamma_y)}{1-\gamma_y}\Delta\gamma_y \end{aligned} \tag{36}$$

holds, as the first line of Eq. (36) follows from the monotonicity (33) and the second line follows from the concavity (34) together with property (32) if $0 \leq \gamma_y \leq 1$. Later we will give explicit expressions for the decomposition (35), so that these properties can easily be checked. Fig. (1) illustrates Eq. (36) schematically.

Moreover, the approximation of Eq. (36) can simplified further, if one could find a parameter $\tilde{\gamma}$ independent of y with the properties $\tilde{\gamma} \geq \gamma_y$ and $\tilde{\gamma} \leq 1$, as

$$\begin{aligned} g(P(0|y),\gamma_y) &\geq g\,(P(0|y),\tilde{\gamma}) \\ \frac{g\,(P(0|y),\gamma_y)}{1-\gamma_y} &\leq \frac{g\,(P(0|y),\tilde{\gamma})}{1-\tilde{\gamma}} \ . \end{aligned} \tag{37}$$

We will see later that setting $\tilde{\gamma}$ to γ as defined in Eq. (27) satisfies these constraints. The first bound of (37) is a simple consequence of the monotonicity (33), whereas the second inequality follows from the properties (32–34). It can easily be verified by realizing that the quantity $\frac{g(P(0|y),\Gamma_y)}{1-\Gamma_y}$ is given by the modulus of the gradient of the straight line connecting the points $g\,(P(0|y),\Gamma_y)$ and $g\,(P(0|y),\Gamma_y=1)=0$. From Fig. 1 it is obvious that this modulus increases if one chooses the point Γ_y to be closer to one. Therefore, the second bound of (37) is valid for all $\tilde{\gamma}$ satisfying $\gamma_y \leq \tilde{\gamma} \leq 1$. Finally, we can estimate the conditional entropy $S(E|Y)$ given by Eq. (28) with the help of the expressions (36) and (37) as

$$\begin{aligned} S(E|Y) &= \int dy P(y) S(\rho_E^y) \\ &\geq \int dy P(y) g(P(0|y),\tilde{\gamma}) \\ &\quad - \frac{1}{1-\tilde{\gamma}} \int dy P(y) g(P(0|y),\tilde{\gamma}) \Delta\gamma_y \ . \\ &= \int dy P(y) g(P(0|y),\tilde{\gamma}) - \Delta S \ , \end{aligned} \tag{38}$$

where we introduced the term ΔS as a shorthand notation.

In the following, we will give explicit expressions for the missing parameters γ_y, $\Delta\gamma_y$ and $\tilde{\gamma}$ in order to connect these parameters to quantities that are observable to Alice and Bob. The starting point of this analysis is again noticing that the state $|\Psi_{BE}^x\rangle$ that Bob and Eve share conditioned on Alice's measurement outcome x is pure, so that one can decompose it as

$$|\Psi_{BE}^x\rangle = \sqrt{(1-\tilde{\varepsilon}_x)}|\tilde{\beta}_x\rangle|\tilde{\varepsilon}_x\rangle + \sqrt{\tilde{\varepsilon}_x}|\varphi_{EB}^x\rangle \ , \tag{39}$$

using Schmidt's decomposition theorem [23]. We have introduced eigenstate $|\tilde{\beta}_x\rangle$ of Bob's conditional density matrix ρ_B^x corresponding to the maximal eigenvalue $1-\tilde{\varepsilon}_x$. All terms orthogonal to $|\tilde{\beta}_x\rangle|\tilde{\varepsilon}_x\rangle$ are summed up in the term $|\varphi_{EB}^x\rangle$, such that $\langle\tilde{\beta}_x|\varphi_{EB}^x\rangle = 0$ and $\langle\tilde{\varepsilon}_x|\varphi_{EB}^x\rangle = 0$. From Eq. (39), one can construct Eve's states $|\Psi_E^{xy}\rangle$ conditioned on both Alice's and Bob's measurement outcomes as

$$|\Psi_E^{xy}\rangle = \frac{\sqrt{(1-\tilde{\varepsilon}_x)}\langle y|\tilde{\beta}_x\rangle|\tilde{\varepsilon}_x\rangle + \sqrt{\tilde{\varepsilon}_x}\langle y_B|\varphi_{EB}^x\rangle}{\sqrt{P(y|x)}} \ . \tag{40}$$

by projecting Bob's system onto $|y\rangle_B\langle y|$. The conditional probabilities $P(y|x)$ are given by

$$P(y|x) = (1-\tilde{\varepsilon}_x)|\langle y|\tilde{\beta}_x\rangle|^2 + \tilde{\varepsilon}_x\,|\langle\varphi_{EB}^x|y\rangle_B\langle y|\varphi_{EB}^x\rangle|^2 \ . \tag{41}$$

By setting

$$a_y^x = \frac{\langle y|\tilde{\beta}_x\rangle}{\sqrt{P(y|x)}} \tag{42}$$

and

$$b_y^x = \frac{\sqrt{\langle\varphi_{EB}^x|y\rangle_B\langle y|\varphi_{EB}^x\rangle}}{\sqrt{P(y|x)}} \ , \tag{43}$$

we can express Eq.(40) as

$$|\Psi_E^{xy}\rangle = \sqrt{(1-\tilde{\varepsilon}_x)}a_y^x|\tilde{\varepsilon}_x\rangle + \sqrt{\tilde{\varepsilon}_x}b_y^x|\varphi_E^{xy}\rangle, \tag{44}$$

where $|\tilde{\varepsilon}_x\rangle$ is orthogonal to $|\varphi_E^{xy}\rangle$. The normalized states $|\varphi_E^{xy}\rangle$ are given by Eqs. (40), (42), (43) and (44) as

$$|\varphi_E^{xy}\rangle = \left(\langle\varphi_{EB}^x|y\rangle_B\langle y|\varphi_{EB}^x\rangle\right)^{-\frac{1}{2}}\langle y_B|\varphi_{EB}^x\rangle \ . \tag{45}$$

Without loss of generality, we can choose a_y^x and b_y^x to be real. Moreover, from expansion (44) it is obvious that

$$\sqrt{1-\tilde{\varepsilon}_x}a_y^x \leq 1 \tag{46}$$

holds. The overlap Γ_y is given by Eq. (44) as

$$\begin{aligned}\Gamma_y =& \left|\langle\Psi_E^{0y}|\Psi_E^{1y}\rangle\right| \\ =& \Big|\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}a_y^0 a_y^1\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle \\ &+ \sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}a_y^0 b_y^1\langle\tilde{\varepsilon}_0|\varphi_E^{1y}\rangle \\ &+ \sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}b_y^0 a_y^1\langle\varphi_E^{0y}|\tilde{\varepsilon}_1\rangle \\ &+ \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1\langle\varphi_E^{0y}|\varphi_E^{1y}\rangle\Big| \ ,\end{aligned} \tag{47}$$

so that Eq. (35) follows from (47) by triangle inequality with the parameters γ_y and $\Delta\gamma_y$ defined as

$$\begin{aligned}\gamma_y =& \left|\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}a_y^0 a_y^1\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle\right| \\ =& \left|\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}a_y^0 a_y^1\right|\gamma \\ \Delta\gamma_y =& \Big|\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}a_y^0 b_y^1\langle\tilde{\varepsilon}_0|\varphi_E^{1y}\rangle \\ &+ \sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}b_y^0 a_y^1\langle\varphi_E^{0y}|\tilde{\varepsilon}_1\rangle \\ &+ \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1\langle\varphi_E^{0y}|\varphi_E^{1y}\rangle\Big| \ .\end{aligned} \tag{48}$$

With the help of Eq. (46), the parameter γ_y can be upper bounded as

$$\gamma_y = \left|\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}a_y^0 a_y^1\right|\gamma \leq \gamma \ , \tag{49}$$

so that we can set

$$\tilde{\gamma} = \gamma \tag{50}$$

to satisfy $\gamma_y \leq \tilde{\gamma}$. Moreover, it can easily be checked that $0 \leq \gamma_y \leq \gamma \leq 1$ using property (46).

In principle, we have now everything at hand to lower bound the conditional entropy $S(E|Y)$ according to Eq. (38). However, as we will see later, we can only estimate the overlap $\gamma = |\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle|$ and eigenvalues $1-\tilde{\varepsilon}_x$ from Bob's measurements. As a consequence, the parameter $\Delta\gamma_y$ cannot be estimated by the observation and consequently the term ΔS in Eq. (38) cannot computed directly. Since ΔS is monotone in the parameter $\Delta\gamma_y$, it is again possible to lower bound the entropy $S(E|Y)$ by looking for a suitable upper bound for $\Delta\gamma_y$ which is a function of Bob's observable parameters. Here, we estimate the parameter $\Delta\gamma_y$ starting from the definitions (48) as

$$\begin{aligned}\Delta\gamma_y \leq& \left|\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}a_y^0 b_y^1\right|\left|\langle\tilde{\varepsilon}_0|\varphi_E^{1y}\rangle\right| \\ &+ \left|\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}a_y^1 b_y^0\right|\left|\langle\tilde{\varepsilon}_1|\varphi_E^{0y}\rangle\right| \\ &+ \left|\sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1\right|\left|\langle\varphi_E^{0y}|\varphi_E^{1y}\rangle\right| \\ \leq& \sqrt{(1-\tilde{\varepsilon}_0)\,\tilde{\varepsilon}_1}a_y^0 b_y^1\sqrt{1-|\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle|^2} \\ &+ \sqrt{(1-\tilde{\varepsilon}_1)\,\tilde{\varepsilon}_0}a_y^1 b_y^0\sqrt{1-|\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle|^2} \\ &+ \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1 \\ \leq& \sqrt{1-\gamma^2}\left(\sqrt{\tilde{\varepsilon}_1}b_y^1 + \sqrt{\tilde{\varepsilon}_0}b_y^0\right) + \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1\end{aligned} \tag{51}$$

where we first used the triangle inequality. For the second inequality in Eq. (51) we used $\left|\langle\varphi_E^{0y}|\varphi_E^{1y}\rangle\right| \leq 1$ and

$$|\langle\Phi|\tilde{\varepsilon}_x\rangle|^2 + |\langle\Phi|\varphi_E^{xy}\rangle|^2 \leq 1 \ , \tag{52}$$

which is valid for any vector $|\Phi\rangle$ by orthogonality of the states $|\tilde{\varepsilon}_x\rangle$ and $|\varphi_E^{xy}\rangle$. In particular, we used

$$\begin{aligned}|\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle|^2 + \left|\langle\tilde{\varepsilon}_0|\varphi_E^{1y}\rangle\right|^2 &\leq 1 \\ |\langle\tilde{\varepsilon}_1|\tilde{\varepsilon}_0\rangle|^2 + \left|\langle\tilde{\varepsilon}_1|\varphi_E^{0y}\rangle\right|^2 &\leq 1 \ ,\end{aligned} \tag{53}$$

which follows from Eq. (52) by setting $|\Phi\rangle = |\varepsilon_0\rangle$ and $x=1$ for the first inequality or respectively $|\Phi\rangle = |\varepsilon_1\rangle$ and $x=0$ for the last inequality in Eq. (53). In the last step of Eq. (51), we used the definition (27) of γ and the bound (46).

With the expression (51), we can upper bound the term ΔS of Eq.(38) as

$$\begin{aligned}\Delta S \leq& \sqrt{\frac{1+\gamma}{1-\gamma}}\int dyP(y)g(P(0|y),\gamma)\left(\sqrt{\tilde{\varepsilon}_0}b_y^0 + \sqrt{\tilde{\varepsilon}_1}b_y^1\right) \\ &+ \frac{1}{1-\gamma}\int dyP(y)g(P(0|y),\gamma)\left(\sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1\right) .\end{aligned} \tag{54}$$

These integrals can be estimated first applying the completeness relation $\int dy|y\rangle\langle y| = I$ of Bob's homodyne measurement to the definition (43). It follows that

$$\int dyP(y|x)b_y^{x\,2} = \int dy\langle\varphi_{EB}^x|y\rangle_B\langle y|\varphi_{EB}^x\rangle = 1 \ . \tag{55}$$

This condition on the parameters b_y^x enables us to upper bound the remaining terms in Eq. (54) as

$$\begin{aligned}&\int dyP(y)g(P(0|y),\gamma)\sqrt{\tilde{\varepsilon}_x}b_y^x \\ \leq& \sqrt{\frac{\tilde{\varepsilon}_x}{2}\int dyP(y)\frac{g^2(P(0|y),\gamma)}{P(x|y)}},\end{aligned} \tag{56}$$

and

$$\int dyP(y)g(P(0|y),\gamma)\sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}b_y^0 b_y^1 \leq \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}g\left(\frac{1}{2},\gamma\right) \ . \tag{57}$$

with the help of the Cauchy-Schwarz-Buniakovsky inequality [27]. Details of this estimation can be found in Appendix A.

Let us summarize our results. We can use Eq. (50) in Eq. (38) to bound the conditional entropy $S(E|Y)$ as

$$S(E|Y) \geq \int dyP(y)g\left(P(0|y),\gamma\right) - \Delta S \ . \tag{58}$$

It follows from the inequalities (54), (56) and (57) that the term ΔS can be upper bounded as

$$\Delta S \leq \tilde{\varepsilon}_0 k_0 + \tilde{\varepsilon}_1 k_1 + \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}\tilde{k} \ , \tag{59}$$

where we defined parameters k_x and $\tilde{k}$ as

$$\begin{aligned} k_x &= \sqrt{\frac{1+\gamma}{2(1-\gamma)}\int dyP(y)\frac{g^2\left(P(0|y),\gamma\right)}{P(x|y)}} \\ \tilde{k} &= \frac{1}{1-\gamma}g\left(\frac{1}{2},\gamma\right) \ . \end{aligned} \tag{60}$$

Finally, a lower bound for the conditional entropy $S(E|Y)$ is therefore given by Eqs. (58) and (54) as

$$\begin{aligned} S(E|Y) \geq & \int dyP(y)g\left(P(0|y),\gamma\right) \\ & - \sqrt{\tilde{\varepsilon}_0}k_0 - \sqrt{\tilde{\varepsilon}_1}k_1 - \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}\tilde{k} \ . \end{aligned} \tag{61}$$

D. The mutual information $S(Y:E)$ between Bob and Eve

We have shown that an upper bound for the mutual information $S(Y:E)$ between Bob and Eve is given by Eq. (10), (12), (26) and (61) as

$$\begin{aligned} S(Y:E) =& S(E|X) + S(X:E) - S(E|Y) \qquad (62) \\ \leq & \frac{1}{2}\sum_x [(1+V_x)\log_2(1+V_x) - V_x\log_2 V_x] \\ & + h\left[\frac{1}{2}(1-\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}\gamma)\right] \\ & - \int dyP(y)g[P(0|y),\gamma] \\ & + \sqrt{\tilde{\varepsilon}_0}k_0 + \sqrt{\tilde{\varepsilon}_1}k_1 + \sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}\tilde{k} \\ =& \frac{1}{2}\sum_x [(1+V_x)\log_2(1+V_x) - V_x\log_2 V_x] \\ & + s(\tilde{\varepsilon}_x,\gamma) \ . \qquad (63) \end{aligned}$$

The first term in Eq. (62) can be directly computed from Bob's observed variances (14) using Eq. (13). Here, we define the function $s(\tilde{\varepsilon}_x,\gamma)$ to summarize all terms that depend on the maximal eigenvalues $1-\tilde{\varepsilon}_x$ and overlap γ of the corresponding eigenstates of Eve's conditional states. The remaining problem is to estimate these parameters via Bob's homodyne measurement.

V. MAXIMAL EIGENVALUE AND EIGENSTATE

We have already shown in the last section that the two party states $|\Psi^x_{BE}\rangle$ conditioned on Alice's measurement outcome x can be chosen to be pure. Therefore, one can expand these conditional states using the Schmidt-decomposition (39), so that the state $|\tilde{\beta}_x\rangle|\tilde{\varepsilon}_x\rangle$ is orthogonal to $|\varphi^x_{EB}\rangle$. From Eq.(39) it follows that the ρ^x_E and ρ^x_B have the same spectrum. Moreover, the eigenvectors of Bob's and Eve's system are determined up to a global unitary operation on Eve's system. According to Eq. (62), we need to estimate the modulus of the overlap of Eve's maximal eigenstates $|\tilde{\varepsilon}_x\rangle$ and the maximal eigenvalues $1-\tilde{\varepsilon}_x$. These parameters can be estimated from the first and second moments of Bob's measured data [20], as we will see in the following.

Suppose the fidelity between Bob's received conditional state ρ^x_B and a pure coherent state $|\overline{\beta}\rangle$ satisfies

$$\langle\overline{\beta}_x|\rho^x_B|\overline{\beta}_x\rangle = 1-\varepsilon_x \ . \tag{64}$$

The amplitude $\overline{\beta}_x$ is given by the first moments of Bob's homodyne measurement as

$$\begin{aligned} \mathrm{Re}(\overline{\beta}_x) &= \mathrm{tr}(\rho^x_B\hat{q}) \\ \mathrm{Im}(\overline{\beta}_x) &= \mathrm{tr}(\rho^x_B\hat{p}) \ . \end{aligned} \tag{65}$$

The quadrature operators $\hat{q}$ and $\hat{p}$ are defined in Eq. (16). In the following, we will refer to the parameter ε_x as the mixedness of Bob's conditional states.

It has been shown by Rigas [20] that the mixedness ε_x of the conditional states can be upper bounded from the outcomes of a homodyne measurement as

$$\varepsilon_x \leq \frac{1}{2}\left[(V^2_{Y_q|x}+\frac{1}{2})(V^2_{Y_p|x}+\frac{1}{2})-1\right] = U_x, \tag{66}$$

where $V_{Y_q|x}$ and $V^2_{Y_p|x}$ denote the variances of the q- and p-quadrature distributions (14) conditioned on Alice's variable x. The proof for the estimation (66) is given in Appendix (B). Moreover, one can also estimate the overlap $|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle|$ of Bob's maximal conditional eigenstates as

$$c_l(\tilde{\varepsilon}_x,\varepsilon_x,\kappa) \leq |\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle| \leq c_u(\tilde{\varepsilon}_x,\varepsilon_x,\kappa) \ , \tag{67}$$

if one assumes that the fidelity (64) is given. Here, the parameter κ is given by the overlap of the coherent states corresponding to the mean values (65) as

$$\kappa = \left|\langle\overline{\beta}_0|\overline{\beta}_1\rangle\right| \ . \tag{68}$$

The detailed expression of $c_l(\tilde{\varepsilon}_x, \varepsilon_x, \kappa)$ and $c_u(\tilde{\varepsilon}_x, \varepsilon_x, \kappa)$ can be seen in Appendix C.

The results (66) and (67) can be used to estimate the maximal eigenvalues and overlap γ of the corresponding eigenstates of Eve's reduced density matrix. From the Schmidt decomposition (39) it follows that the eigenvalues of Bob's and Eve's reduced conditional density matrices are identical, so that

$$\tilde{\varepsilon}_x \leq \varepsilon_x \tag{69}$$

can easily be seen by expanding ρ_B^x in its eigenbasis. Moreover, Eve's attack should preserve the inner product [3], so that $\langle -\alpha|\alpha\rangle = \langle \Psi_{BE}^0 | \Psi_{BE}^1 \rangle$. In Appendix D we show that this allows us to bound the overlap γ of Eve's eigenstates as

$$d_l \leq \gamma \leq d_u \ , \tag{70}$$

where

$$d_l = \frac{|\langle -\alpha|\alpha\rangle| - \sqrt{[\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0} + \sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}]^2 + \tilde{\varepsilon}_1\tilde{\varepsilon}_0}}{\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}\, c_u(\tilde{\varepsilon}_x, \varepsilon_x, \kappa)} \tag{71}$$

and

$$d_u = \frac{|\langle -\alpha|\alpha\rangle| + \sqrt{[\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0} + \sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}]^2 + \tilde{\varepsilon}_1\tilde{\varepsilon}_0}}{\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}\, c_l(\tilde{\varepsilon}_x, \varepsilon_x, \kappa)} \ . \tag{72}$$

The functions $c_l(\tilde{\varepsilon}_x, \varepsilon_x, \kappa)$ and $c_u(\tilde{\varepsilon}_x, \varepsilon_x, \kappa)$ are the extremal values of the overlap $\left|\langle \tilde{\beta}_0 | \tilde{\beta}_1 \rangle\right|$ of Bob's maximal eigenstates as defined in Eq. (67).

If the first and second moments of Bob's measurement outcomes are fixed, U_x is given by Eq. (66). Therefore, the parameters $\tilde{\varepsilon}_x$ that are compatible with the observed data can vary between $0 \leq \tilde{\varepsilon}_x \leq \varepsilon_x \leq U_x$. In that respect, the quantities ε_x and $\tilde{\varepsilon}_x$ are interior parameters that can only be bounded by the value of the observable quantity U_x. For any given value of ε_x, $\tilde{\varepsilon}_x$ and κ, the interval of compatible overlaps $|\langle \tilde{\beta}_0 | \tilde{\beta}_1 \rangle|$ according to Eq. (67) can be given. This in turn determines the interval of possible overlaps γ via Eq. (70). The value for κ is obtainable from the first moments of Bob's homodyne measurement, as can be seen from Eq. (65). Finally, the secret key rate can be obtained by

$$\begin{aligned} G \geq & I(X:\tilde{Y}|U) - \max_{\substack{0 \leq \tilde{\varepsilon}_x \leq \varepsilon_x \leq U_x \\ d_l \leq \gamma \leq d_u}} \{ s(\tilde{\varepsilon}_x, \gamma) \\ & - \frac{1}{2}\sum_x [(1+V_x)\log_2(1+V_x) - V_x \log_2 V_x]\} \ . \end{aligned} \tag{73}$$

The maximum is taken over the interior parameters $\tilde{\varepsilon}_x$, ε_x and γ satisfying the bounds shown. These interior parameters can vary in intervals that are fixed by the values of U_x and κ that can be determined from the observation. As the s-function (62) contains details about Bob's measured data via the probability distributions $P(y)$ and $P(0|y)$, this additional information must be estimated from the measured data to analyze the secret key rate numerically for a given observation.

VI. NUMERICAL RESULTS

The secret key rate (73) depends on Bob's observed probability distributions $P(y|x)$ directly via the mutual information term $I(X:\tilde{Y}|U)$ between Alice and Bob and via the term $s(\tilde{\varepsilon}_x, \gamma)$, as can be seen from Eq. (62). The distribution $P(y|x)$ is in principle available from experiments. To evaluate the secret key rate in an example, we simulate data for a typical experimental situation in which we find a Gaussian distribution [7, 8, 15]. Therefore, we choose the probability distribution $P(y|x)$ to be parameterized as

$$P(y|x) = \frac{1}{\sqrt{2\pi V_{Y_q|x}^2}} \exp\left[\frac{-(\sqrt{\eta}\alpha_x - y)^2}{2V_{Y_q|x}^2}\right] \ . \tag{74}$$

Here, η is the observed channel transmission, the amplitude $\alpha_0 = -\alpha_1$ is chosen to be real. In this parameterization, the value of κ as defined in Eq. (68) is given by by the loss of the quantum channel and the overlap of Alice's input states as

$$\kappa = |\langle \sqrt{\eta}\alpha| - \sqrt{\eta}\alpha\rangle| \ . \tag{75}$$

Furthermore, we assume that Bob observes the same variance (14) in his measured data for both the q- and the p- quadratures, so that

$$V_{Y_q|x}^2 = V_{Y_p|x}^2 \ . \tag{76}$$

Here, we use the convention for the excess noise δ given in Ref. [28]:

$$\delta = \frac{V_{Y_q|x}^2}{V_{Y_q|x,\text{Vac}}^2} - 1 \tag{77}$$

The quantity $V_{Y_q|x,\text{Vac}}^2 = \frac{1}{2}$ is the quadrature variance of the vacuum state. As the *a priori* probabilities $p(x) = \frac{1}{2}$ are fixed, the probability distribution $p(y)$ is can easily be evaluated with the help of (74) and the secret key rate can be evaluated according to (73). Fig. (2) shows our numerical results for the secret key rate versus the loss $1-\eta$ and different values for the excess noise δ in this typical scenario.

For the simulation, we assume that Bob announces the modulus of his measurement outcomes y as $u = |y|$. The values of $\tilde{y}$ are determined by the map $\tilde{y} = 0$ if $y < 0$ and $\tilde{y} = 1$ otherwise. After the announcement, the conditional mutual information between Alice and Bob is

$$\begin{aligned} I(X:\tilde{Y}|U) &= H(X|U) + H(X|\tilde{Y}U) \\ &= H(X) - H(X|Y) \\ &= I(X:Y) \ . \end{aligned} \tag{78}$$

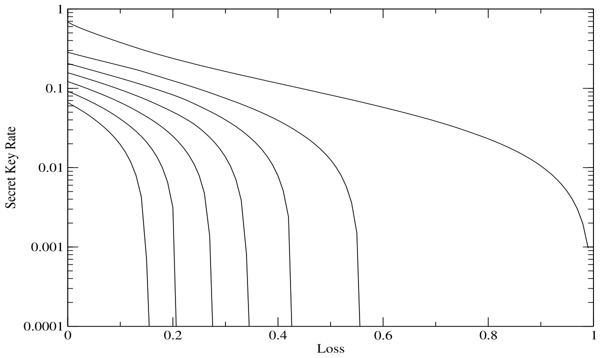

FIG. 2: Secret key rate versus channel loss for a typical scenario with optimized signal strength. The different lines correspond to an excess noise δ of $\{0, 0.0004, 0.0008, 0.0012, 0.0016, 0.0020, 0.0024\}$.

The announcement $u = |y|$ contains no information about the bit-value x for symmetric probability distributions like (74) as the conditional probability $p(u|x)$ for a particular announcement u is independent of x. Therefore it follows that $H(X|U) = H(X)$. The knowledge of Bob's measured outcome y is obviously equivalent to the knowledge of $u = |y|$ and the sign of y, so that we have $H(X|\tilde{Y}U) = H(X|Y)$. Therefore, we can achieve $I(X : \tilde{Y}|U) = I(X : Y)$ with this simple map as long as the probability distribution satisfies the symmetry condition $p(x|u) = 1/2$.

For the numerical evaluation we optimize the secret key rate G over the overlap $\langle -\alpha|\alpha\rangle$ of the input states. In the optimization we vary α between zero and 1 with step-width 0.05. For each α we find the maximum of $s(\tilde{\varepsilon}_x, \gamma)$ over all $\tilde{\varepsilon}_x \leq \varepsilon_x \leq U_x$ and $d_l \leq \gamma \leq d_u$. We find numerically that the maximum of $s(\tilde{\varepsilon}_x, \gamma)$ is attained at the point $\gamma = d_l$.

Fig. (2) shows the results of our simulation. As we can see, the secret key rate is very susceptible to noise, whereas it coincides with the optimal bound given in Ref. [3] for lossy but noiseless quantum channels. However, one should keep in mind that we only calculated an upper bound for Eve's knowledge, which we expect not to be tight for finite excess noise. We have bounded all three terms in Eq. (10) separately rather than bounding those terms simultaneously. Furthermore, one might expect to find a different purification for the system Q to make the bound (26) tighter. Finally, we have linearized the conditional entropy $S(E|Y)$ in Section III. B in order to be able to find a bound. However, the error introduced here might be quite large.

VII. CONCLUSION

We have evaluated a lower bound to the secret key rate for a binary modulated CV-QKD protocol in the collective attack scenario. The analysis can be applied to any given channel noise, as Alice and Bob can estimate the conditional probability distribution $p(y|x)$ of their measurement outcomes arbitrary well in the limit that the number of exchanged signals tends to infinity. For any given probability distribution, the secret key rate can be computed according to Eq. (73). Although we demonstrate that our approach yields positive secret key rates for the case of small Gaussian excess noise, these results are not satisfying from a practical point of view, as the secret key rates drop quickly with increasing excess noise. Typically, the dominant contribution to the excess noise in CV-QKD experiments originate from noisy detectors. Our numerical results therefore indicate that it is necessary to analyze these kind of schemes in a trusted device scenario, if one wants to drop the assumption of ideal detectors and obtain secret rates of practical relevance. In this scenario, Eve cannot exploit the noise added by the detectors.

There are several options to make the protocol more robust against channel excess noise. One could use more input states in order to test the quantum channel between Alice and Bob more efficiently and consequently limit Eve's possible interaction with the signal states. If one compares the secret key rates of Fig. (2) with those given in Ref. [4] which correspond to a protocol using a Gaussian modulated, continuous set of input states and a quantum channel imposing Gaussian noise onto the signal states, one realizes that the robustness of the secret key rate increases by orders of magnitude. An introduction of a postselection step in the protocol can help to increase the performance as well.

The authors want to thank M. Christandl, M. Razavi, H. Häseler, T. Moroder and G. O. Myhr for helpful discussions. Y.-B. Zhao especially wants to thank Z.-F. Han and G.-C. Guo for supporting his visit to the Institute of Quantum Computing and many fruitful discussions on this topic.

This work was supported by the National Fundamental Research Program of China under Grant No 2006CB921900, the National Natural Science Foundation of China under Grants No. 60537020 and 60621064, the Knowledge Innovation Project of the Chinese Academy of Sciences (CAS), the European Union through the IST Integrated Project SECOQC, the NSERC Innovation Platform Quantum Works, the NSERC Discovery Grant and the Spanish Research Directorate, Grant FIS2005-06714.

APPENDIX A: CAUCHY-SCHWARZ-BUNIAKOWSKY INEQUALITY

The Cauchy-Schwarz-Buniakowsky inequality states [27] that for any two integrable functions $f(x)$ and $g(x)$

$$\left(\int_a^b dy f(y)h(y)\right)^2 \leq \left(\int_a^b dy f^2(y)\right)\left(\int_a^b dy h^2(y)\right) \tag{A1}$$

holds. Application of inequality (A1) to the left hand side of expression (56) yields

$$\begin{aligned} &\int dy P(y) g[P(0|y),\gamma]\sqrt{\tilde{\varepsilon}_x} b_y^x \\ =\ & \sqrt{\tilde{\varepsilon}_x}\int dy \underbrace{\sqrt{P(y|x)}b_y^x}_{f(y)}\underbrace{\{P(y)g[P(0|y),\gamma]/\sqrt{P(y|x)}\}}_{h(y)} \\ \leq\ & \sqrt{\tilde{\varepsilon}_x}\sqrt{\int dy P(y) g^2[P(0|y),\gamma]\frac{P(y)}{P(y|x)}}. \end{aligned} \tag{A2}$$

Since one can rewrite the conditional probability $P(y|x)$ as $P(y|x) = P(x|y)P(y)/P(x)$ by using Bayes' rule and the *a priori* probabilities are given by $P(x) = \frac{1}{2}$, we have

$$\frac{P(y)}{P(y|x)} = \frac{1}{2P(x|y)} \tag{A3}$$

and inequality (56) follows from Eq. (A2) and Eq. (A3).

Similarly, one can evaluate the left hand side of Eq. (57) with the condition (55) as

$$\begin{aligned} &\int dy P(y) g\left[P(0|y)\gamma\right]\sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1} b_y^0 b_y^1 \qquad \text{(A4)} \\ =\ & \sqrt{\tilde{\varepsilon}_0}\sqrt{\tilde{\varepsilon}_1}\int dy \underbrace{\sqrt{P(y|1)}b_y^1}_{f(y)}\underbrace{\{P(y)g[P(0|y),\gamma]/\sqrt{P(y|1)}\}}_{h(y)} \\ \leq\ & \frac{\sqrt{\tilde{\varepsilon}_0\tilde{\varepsilon}_1}}{2}\sqrt{\int dy P(y|0){b_y^0}^2\frac{g^2\left[P(0|y),\gamma\right]}{P(0|y)P(1|y)}}, \end{aligned}$$

where we used Eq. (A3) again in the last step. Furthermore one can show that

$$\begin{aligned} &\int dy P(y|0){b_y^0}^2\frac{g^2\left[P(0|y),\gamma\right]}{P(0|y)P(1|y)} \\ &\leq \max_y\left\{\frac{g^2\left[P(0|y),\gamma\right]}{P(0|y)P(1|y)}\right\} \\ &= 4g^2\left[\frac{1}{2},\gamma\right] . \end{aligned} \tag{A5}$$

The first line of Eq. (A5) again follows from the boundary condition (55) for any integrable and bounded function $\frac{g_y^2(\gamma)}{P(0|y)P(1|y)}$. The second step can be shown by an involved but straight forward calculation. Eq. (57) now follows from Eqs. (A4) and (A5).

APPENDIX B: ESTIMATION OF THE MIXEDNESS ε_x VIA HOMODYNE MEASUREMENTS

In this Appendix, we prove that the parameter ε_x as defined in Eq. (64) can be estimated via Bob's homodyne measurements as

$$\varepsilon_x \leq \frac{1}{2}\left[\left(V^2_{y_q|x}+\frac{1}{2}\right)\left(V^2_{y_p|x}+\frac{1}{2}\right)-1\right] = \frac{1}{2}(W-1) . \tag{B1}$$

The mixedness ε_x is given by the fidelity between Bob's received state ρ_B^x and the pure coherent state $\overline{\beta_x}$ as

$$\langle\overline{\beta}_x|\rho_B^x|\overline{\beta}_x\rangle = 1-\varepsilon_x . \tag{B2}$$

The amplitude $\overline{\beta}_x$ is given by Eq. (65) and we use the convention (16) for quadrature operators. The conditional variances $V^2_{y_q|x}$ and $V^2_{y_p|x}$ are then given by

$$\begin{aligned} V^2_{y_q|x} &= \mathrm{tr}\left(\rho_B^x\hat{q}^2\right) - \left[\mathrm{tr}\left(\rho_B^x\hat{q}\right)\right]^2 \\ V^2_{y_p|x} &= \mathrm{tr}\left(\rho_B^x\hat{p}^2\right) - \left[\mathrm{tr}\left(\rho_B^x\hat{p}\right)\right]^2 \end{aligned} \tag{B3}$$

Let us introduce a state $\overline{\rho} = \hat{D}(-\overline{\beta}_x)\rho_B^x\hat{D}(\overline{\beta}_x)$ with zero mean values for the quadrature operators (16) to simplify the analysis. Here $\hat{D}(\overline{\beta}_x)$ denotes the displacement operator according to the amplitude $\overline{\beta}_x$. Obviously,

$$\langle\overline{\beta}|\rho_B^x|\overline{\beta}\rangle = \langle 0|\overline{\rho}|0\rangle = 1-\varepsilon_x \tag{B4}$$

holds, whereas $|0\rangle$ denotes the vacuum state. The variances (B3) can now be evaluated with the definition (16) as

$$\begin{aligned} V^2_{y_q|x} &= \mathrm{tr}\left(\overline{\rho}\hat{q}^2\right) = \frac{1}{2}\mathrm{tr}\left[\overline{\rho}\left(2\hat{n}+1+\hat{a}^2+\hat{a}^{\dagger 2}\right)\right] \qquad \text{(B5)} \\ V^2_{y_p|x} &= \mathrm{tr}\left(\overline{\rho}\hat{p}^2\right) = \frac{1}{2}\mathrm{tr}\left[\overline{\rho}\left(2\hat{n}+1-\hat{a}^2-\hat{a}^{\dagger 2}\right)\right] , \end{aligned}$$

where we have introduced the photon number operator $\hat{n} = \hat{a}^\dagger\hat{a}$ as short hand notation. The quantity W in Eq. (B1) now reads

$$\begin{aligned} W =& \frac{1}{4}\mathrm{tr}\left[\overline{\rho}\left(2\hat{n}+2+\hat{a}^2+\left(\hat{a}^\dagger\right)^2\right)\right] \\ &\times \mathrm{tr}\left[\overline{\rho}\left(2\hat{n}+2-\hat{a}^2-\left(\hat{a}^\dagger\right)^2\right)\right] \\ =& \left[\mathrm{tr}\left(\overline{\rho}\hat{n}\right)+1\right]^2 - \frac{1}{4}\mathrm{tr}\left[\overline{\rho}\left(\hat{a}^2+\hat{a}^{\dagger 2}\right)\right]^2 . \end{aligned} \tag{B6}$$

We proceed in rewriting the last term in (B6) with the help of Eqs. (B5) in the Fock-basis $\{|n\rangle\}_n$ as

$$\begin{aligned} \mathrm{tr}\left[\overline{\rho}\left(\hat{a}^2+\hat{a}^{\dagger 2}\right)\right] =& \sum_{n=0}^{\infty}\sqrt{n+2}\sqrt{n+1}\langle n+2|\overline{\rho}|n\rangle \qquad \text{(B7)} \\ &+ \sum_{n=2}^{\infty}\sqrt{n}\sqrt{n-1}\langle n-2|\overline{\rho}|n\rangle \\ =& 2\sum_{n=0}^{\infty}\sqrt{n+2}\sqrt{n+1}\mathrm{Re}\langle n+2|\overline{\rho}|n\rangle . \end{aligned}$$

Since $\langle i|\overline{\rho}|j\rangle$ is a positive semidefinite matrix, any principal minor is a positive semidefinite matrix. It follows that

$$\langle i|\overline{\rho}|i\rangle\langle j|\overline{\rho}|j\rangle - |\langle i|\overline{\rho}|j\rangle|^2 \geq 0 \ , \tag{B8}$$

as this can be interpreted as the determinant of the 2 by 2 principal minor that arises by only keeping the i-th and j-th entries. The positivity of this determinant then follows by realizing that the determinant is just the product of the non-negative eigenvalues of the corresponding principal minor [29]. The result (B8), together with the triangle inequality, can be used to estimate the modulus of Eq. (B7) as

$$\begin{aligned} \left|\mathrm{tr}\left[\overline{\rho}\left(\hat{a}^2+\hat{a}^{\dagger 2}\right)\right]\right| \leq & 2\sum_{n=0}^{\infty}\sqrt{n+2}\sqrt{n+1}\sqrt{\langle n|\overline{\rho}|n\rangle} \qquad \text{(B9)} \\ & \times\sqrt{\langle n+2|\overline{\rho}|n+2\rangle} \\ \leq & 2\sqrt{\sum_{n=0}^{\infty}(n+1)\langle n|\overline{\rho}|n\rangle} \\ & \times\sqrt{\sum_{n=0}^{\infty}(n+2)\langle n+2|\overline{\rho}|n+2\rangle} \\ = & 2\sqrt{\mathrm{tr}\left(\overline{\rho}\hat{n}\right)+1}\sqrt{\mathrm{tr}\left(\overline{\rho}\hat{n}\right)-\langle 1|\overline{\rho}|1\rangle} \ . \qquad \text{(B10)} \end{aligned}$$

The second estimation in Eq. (B9) follows from the Cauchy-Schwarz inequality. Inserting this result into Eq. (B6) yields

$$W \geq \left[\mathrm{tr}\left(\overline{\rho}\hat{n}\right)+1\right]\left[1+\langle 1|\overline{\rho}|1\rangle\right] \ . \tag{B11}$$

We need to find a lower bound on Eq. (B11) depending only on ε_x. Note that $\mathrm{tr}\left(\overline{\rho}\hat{n}\right)$ can be written as

$$\begin{aligned} \mathrm{tr}\left(\overline{\rho}\hat{n}\right) = & \langle 1|\overline{\rho}|1\rangle + \sum_{n=2}^{\infty}\langle n|\overline{\rho}|n\rangle n \qquad \text{(B12)} \\ \geq & \langle 1|\overline{\rho}|1\rangle + 2\left(\varepsilon_x - \langle 1|\overline{\rho}|1\rangle\right) \ . \end{aligned}$$

As it can be seen from Eq. (B4), the fidelity of $\overline{\rho}$ with the vacuum is $1-\varepsilon_x$. It follows that all matrix elements $\langle n|\overline{\rho}|n\rangle$ for $n \geq 1$ sum up to ε_x, so that $\sum_{n=2}^{\infty}\langle n|\overline{\rho}|n\rangle n$ is minimal if all $\langle n|\overline{\rho}|n\rangle = 0$ except for $\langle 2|\overline{\rho}|2\rangle$, which has then to be equal to $\varepsilon_x - \langle 1|\overline{\rho}|1\rangle$ by the summing condition. Therefore, Eq. (B11) can be estimated as

$$\begin{aligned} W & \geq \left(1+2\varepsilon_x-\langle 1|\overline{\rho}|1\rangle\right)\left(1+\langle 1|\overline{\rho}|1\rangle\right) \qquad \text{(B13)} \\ & = 1+2\varepsilon_x+\langle 1|\overline{\rho}|1\rangle(2\varepsilon_x-\langle 1|\overline{\rho}|1\rangle) \ , \end{aligned}$$

As $0 \leq \langle 1|\overline{\rho}|1\rangle \leq \varepsilon_x$, the last term of Eq. (B13) is never negative and equal to zero iff $\langle 1|\overline{\rho}|1\rangle = 0$. It follows that

$$W \geq 1+2\varepsilon_x \ . \tag{B14}$$

Inserting this result into Eq. (B1) concludes the proof.

APPENDIX C: ESTIMATION TO THE OVERLAP OF BOB'S MAXIMAL EIGENSTATES

In the following, we derive explicit expressions for the bounds to the overlap $|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle$ of Bob's conditional eigenstates to the maximal eigenvalue $1-\tilde{\varepsilon}_x$ as given by expression (67). Assume that we know the fidelity

$$\langle\overline{\beta}_x|\rho_B^x|\overline{\beta}_x\rangle = 1-\varepsilon_x \tag{C1}$$

of Bob's received state ρ_B^x with the coherent state $|\overline{\beta_x}\rangle$ is given. The amplitude $\overline{\beta_x}$ is defined in Eq. (65). We can express the conditional states ρ_B^x in a natural basis of displaced Fock-states $\{|\phi_k^x\rangle\} = \{D(\overline{\beta}_x)|k\rangle\}$. Here, the the parameter k labels the photon number. Obviously, $|\overline{\beta}_x\rangle = |\phi_0^x\rangle$ holds. In this basis, ρ_B^x reads

$$\rho_B^x = \begin{bmatrix} a_{00} & a_{01} & \cdots \\ a_{01}^* & a_{11} & \\ \vdots & & \ddots \end{bmatrix} = V^x D^x V^{x\dagger} \ , \tag{C2}$$

where V^x denotes a unknown unitary matrix and D^x is the representation of ρ_B^x in its eigenbasis. Without loss of generality, we can choose the first element in the D-Matrix to correspond to the biggest eigenvalue, so that

$$D_{00}^x = 1-\tilde{\varepsilon}_x \ . \tag{C3}$$

From Eq. (C2), we know that

$$1-\varepsilon_x = a_{00} = |V_{00}^x|^2 D_{00}^x + \sum_{k=1}^{\infty}|V_{0k}^x|^2 D_{kk}^x \tag{C4}$$

As V^x is unitary, it follows that

$$\sum_{k=1}^{\infty}|V_{0k}^x|^2 = 1-|V_{00}^x|^2 \ . \tag{C5}$$

Moreover, D^x is normalized, so that

$$\sum_{k=1}^{\infty}D_{kk}^x = 1-D_{00}^x = \tilde{\varepsilon}_x \ , \tag{C6}$$

where we used Eq. (C3). This can be used to bound the infinite sum in Eq. (C4) as

$$\sum_{k=1}^{\infty}|V_{0k}^x|^2 D_{kk}^x \leq \left(1-|V_{00}^x|^2\right)\tilde{\varepsilon}_x \ , \tag{C7}$$

since all terms $|V_{0k}^x|^2$ and D_{kk}^x appearing in the sum are strictly positive. Therefore, we can bound Eq. (C4) according to inequality (C7) as

$$\begin{aligned} 1-\varepsilon_x & \leq |V_{00}^x|^2\left(1-\tilde{\varepsilon}_x\right) + \left(1-|V_{00}^x|^2\right)\tilde{\varepsilon}_x \\ & = |V_{00}^x|^2\left(1-2\tilde{\varepsilon}_x\right) + \tilde{\varepsilon}_x \ . \end{aligned}$$

It follows that

$$|V_{00}^x|^2 \geq \frac{1-\varepsilon_x-\tilde{\varepsilon}_x}{1-2\tilde{\varepsilon}_x}\ . \tag{C8}$$

Moreover, one can use Eq. (C4) to obtain a lower bound on $|V_{00}^x|^2$ as

$$1-\varepsilon_x \geq |V_{00}^x|^2\left(1-\tilde{\varepsilon}_x\right)\ , \tag{C9}$$

so that

$$|V_{00}^x|^2 \leq \frac{1-\varepsilon_x}{1-\tilde{\varepsilon}_x}\ . \tag{C10}$$

On the other hand, Bob's conditional states can be written as

$$\begin{aligned}\rho_B^0 &= V^0 D^0 {V^0}^\dagger \\ \rho_B^1 &= U V^1 D^1 {V^1}^\dagger U^\dagger\ ,\end{aligned} \tag{C11}$$

where the unitary operation U is given, up to an unimportant unimodular phase, by $U=\hat{D}\left(\overline{\beta}_1\right)\hat{D}\left(-\overline{\beta}_0\right)$ and $\hat{D}$ denotes the displacement operator. Let us denote the eigenvectors of Bob's conditional states ρ_B^x as $\{|\tilde{\beta}_l^x\rangle\}$ with $|\tilde{\beta}_x\rangle$ being the eigenstate corresponding to the biggest eigenvalue $1-\tilde{\varepsilon}_x$. With the representation (C11), these states can be written as

$$\begin{aligned}|\tilde{\beta}_0\rangle &= V^0|\phi_0^0\rangle \\ |\tilde{\beta}_1\rangle &= UV^1|\phi_0^0\rangle\ ,\end{aligned} \tag{C12}$$

so that

$$\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle = \sum_{k,j=0}^{\infty} {V_{k0}^0}^* U_{kl} V_{l0}^1 \tag{C13}$$

By use of the triangle inequalities, one can construct an upper bound as

$$\begin{aligned}\left|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\right| \leq{}& |U_{00}|\left|V_{00}^0\right|\left|V_{00}^1\right| + \left|V_{00}^0\right|\left|\sum_{l=1}^{\infty} U_{0l}V_{l0}^1\right| \\ &+ \left|V_{00}^1\right|\left|\sum_{k=1}^{\infty} U_{k0}{V_{k0}^0}^*\right| + \left|\sum_{k,l=1}^{\infty} {V_{k0}^0}^* U_{kl} V_{l0}^1\right|\end{aligned} \tag{C14}$$

and a lower bound as

$$\begin{aligned}\left|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\right| \geq{}& |U_{00}|\left|V_{00}^0\right|\left|V_{00}^1\right| - \left|V_{00}^0\right|\left|\sum_{l=1}^{\infty} U_{0l}V_{l0}^1\right| \\ &- \left|V_{00}^1\right|\left|\sum_{k=1}^{\infty} U_{k0}{V_{k0}^0}^*\right| - \left|\sum_{k,l=1}^{\infty} {V_{k0}^0}^* U_{kl} V_{l0}^1\right|\ .\end{aligned} \tag{C15}$$

Upper bounds on the sums in Eqs.(C14) and (C15) can be obtained by using the Cauchy-Schwarz inequality as

$$\begin{aligned}\sum_{k=1}^{\infty}|U_{k0}|\left|V_{k0}^0\right| &\leq \sqrt{1-|U_{00}|^2}\sqrt{1-|V_{00}^0|^2} \\ \sum_{l=1}^{\infty}|U_{0l}|\left|V_{l0}^1\right| &\leq \sqrt{1-|U_{00}|^2}\sqrt{1-|V_{00}^1|^2} \\ \left|\sum_{k,l=1}^{\infty} {V_{k0}^0}^* U_{kl} V_{l0}^1\right| &\leq \sqrt{1-|V_{00}^0|^2}\sqrt{1-|V_{00}^1|^2}\ .\end{aligned} \tag{C16}$$

It is easy to see that $|U_{00}| = |\langle\overline{\beta}_0|\overline{\beta}_1\rangle| := \kappa$. Finally, inserting Eqs. (C8, C10, C16) in Eq. (C14) yields

$$\begin{aligned}\left|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\right| \leq{}& \kappa\sqrt{\frac{1-\varepsilon_0}{1-\tilde{\varepsilon}_0}}\sqrt{\frac{1-\varepsilon_1}{1-\tilde{\varepsilon}_1}} \\ &+ \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_0}{1-\tilde{\varepsilon}_0}}\sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}} \\ &+ \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_1}{1-\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}} \\ &+ \sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}}\ .\end{aligned} \tag{C17}$$

Similarly, a lower bound can be obtained by Eqs. (C8, C10, C16) and (C15) as

$$\begin{aligned}\left|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\right| \geq{}& \kappa\sqrt{\frac{1-\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}}\sqrt{\frac{1-\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}} \\ &- \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_0}{1-\tilde{\varepsilon}_0}}\sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}} \\ &- \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_1}{1-\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}} \\ &- \sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}}\ .\end{aligned} \tag{C18}$$

The explicit expression for $c_l\left(\tilde{\varepsilon}_x,\varepsilon_x,\kappa\right)$ is therefore given by Eq. (C18) and respectively, $c_u\left(\tilde{\varepsilon}_x,\varepsilon_x,\kappa\right)$ is given by Eq. (C17).

APPENDIX D: ESTIMATION TO THE OVERLAP OF EVE'S MAXIMAL EIGENSTATES

In the collective attack scenario, Eve's attack can be modelled by attaching an ancilla system to the signals $|\pm\alpha\rangle$ and performing a unitary operation on the joint system. As any unitary preserves the inner product, the overlap $|\langle\Psi_{BE}^0|\Psi_{BE}^1\rangle|$ of the states after the interaction is given by input overlap $|\langle-\alpha|\alpha\rangle|$. This can be written as

$$\begin{aligned} |\langle -\alpha|\alpha\rangle| &= |\langle \Psi^0_{BE}|\Psi^1_{BE}\rangle| \\ &= |\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle \\ &\quad +\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}\langle\tilde{\beta}_0|\langle\tilde{\varepsilon}_0|\varphi^1_{EB}\rangle \\ &\quad +\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}\langle\varphi^0_{EB}|\tilde{\beta}_1\rangle|\tilde{\varepsilon}_1\rangle \\ &\quad +\sqrt{\tilde{\varepsilon}_1\tilde{\varepsilon}_0}\langle\varphi^0_{EB}|\varphi^1_{EB}\rangle|. \end{aligned} \tag{D1}$$

using decomposition (39), where $|\varphi^x_{EB}\rangle$ is orthogonal to $|\tilde{\beta}_x\rangle|\tilde{\varepsilon}_x\rangle$. This orthogonality can be used to construct the inequalities

$$\begin{aligned} |\langle\varphi^0_{EB}|\varphi^1_{EB}\rangle|^2 + |\langle\varphi^0_{EB}|\tilde{\beta}_1\rangle|\tilde{\varepsilon}_1\rangle|^2 \leq 1 \\ |\langle\varphi^0_{EB}|\varphi^1_{EB}\rangle|^2 + |\langle\tilde{\beta}_0|\langle\tilde{\varepsilon}_0|\varphi^1_{EB}\rangle|^2 \leq 1\ . \end{aligned} \tag{D2}$$

We can estimate the last three terms of the right hand side of Eq. (D1) using the triangle inequality and inequalities (D2) as

$$\begin{aligned} &|\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}\langle\tilde{\beta}_0|\langle\tilde{\varepsilon}_0|\varphi^1_{EB}\rangle \\ &\quad + \sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}\langle\varphi^0_{EB}|\tilde{\beta}_1\rangle|\tilde{\varepsilon}_1\rangle + \\ &\quad + \sqrt{\tilde{\varepsilon}_1\tilde{\varepsilon}_0}\langle\varphi^0_{EB}|\varphi^1_{EB}\rangle| \\ &\leq \underbrace{\sqrt{1-|\langle\varphi^0_{EB}|\varphi^1_{EB}\rangle|^2}}_{x_0}\underbrace{\left(\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}+\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}\right)}_{y_0} \\ &\quad + \underbrace{|\langle\varphi^0_{EB}|\varphi^1_{EB}\rangle|}_{x_1}\underbrace{\sqrt{\tilde{\varepsilon}_1\tilde{\varepsilon}_0}}_{y_1} \\ &\leq \sqrt{[\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}+\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}]^2+\tilde{\varepsilon}_1\tilde{\varepsilon}_0}\ . \end{aligned} \tag{D3}$$

In the sixth line we have use fact the that if $\sum_i x_i^2 = 1$, $\sum_i x_i y_i \leq \sqrt{\sum_i y_i^2}$ holds, which can easily derived from the Cauchy-Schwarz inequality of two vectors in $\mathbb{R}^2$. From Eq. (D3) and Eq. (D1), we obtain

$$\begin{aligned} &|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle| \\ &\geq \frac{|\langle -\alpha|\alpha\rangle| - \sqrt{[\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}+\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}]^2+\tilde{\varepsilon}_1\tilde{\varepsilon}_0}}{\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}}. \end{aligned}$$

and

$$\begin{aligned} &|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle| \\ &\leq \frac{|\langle -\alpha|\alpha\rangle| + \sqrt{[\sqrt{(1-\tilde{\varepsilon}_1)\tilde{\varepsilon}_0}+\sqrt{(1-\tilde{\varepsilon}_0)\tilde{\varepsilon}_1}]^2+\tilde{\varepsilon}_1\tilde{\varepsilon}_0}}{\sqrt{(1-\tilde{\varepsilon}_0)(1-\tilde{\varepsilon}_1)}}. \end{aligned}$$

Finally, we obtain Eqs. (70-72) by inserting the extremal values for the possible overlaps $\left|\langle\tilde{\beta}_0|\tilde{\beta}_1\rangle\right|$ of Bob's maximal eigenstates given by Eq. (67) and the definition $\gamma := |\langle\tilde{\varepsilon}_0|\tilde{\varepsilon}_1\rangle|$.

[1] G. van Assche, S. Iblisbir, and N. J. Cerf, Phys. Rev. A **71**, 052305 (2005).

[2] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).

[3] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[4] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[5] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (06).

[6] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[7] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[8] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[9] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[10] I. Devetak and A. Winter, Proc. of the Roy. Soc. of London Series A **461**, 207 (2005).

[11] R. Renner, Nature Physics **3**, 645 (2007).

[12] M. Christandl and B. Toner, arXiv:0712.0916.

[13] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).

[14] S. K. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).

[15] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, Phys. Rev. A **74**, 042326 (2006).

[16] T. Symul, D. J. Alton, A. S. M., A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303 (2007).

[17] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, et al., Phys. Rev. A **76**, 042305 (2007).

[18] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[19] H. Häseler, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **77**, 032303 (2008).

[20] J. Rigas, *Detection of prepare&measurement entanglement in continuous variable quantum key distribution*, Diplom thesis, University of Erlangen-Nuremberg (2006).

[21] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[22] R. Renner, Ph.D. thesis, ETH Zürich (2005), also avail-

able as arXiv:quant-ph/0512258.

[23] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[24] C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[25] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).

[26] G. S. Agarwal, Phys. Rev. A **3**, 828 (1971).

[27] I. R. Gradshteyn and I. M. Ryzhik, *Table of integrals, series and products* (Academic Press, Boston, 1994), 5th ed.

[28] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).

[29] R. A. Horn and C. R. Johnson, *Matrix analysis* (Cambridge University Press, 1985).